Rotation Scale Invariant Semi Blind Biometric Watermarking Technique for Colour Image

Vandana Inamdar [1], Priti Rege [2], and Chandrama Thorat [3]
[1] College of Engineering, Department of Computer Engineering and IT, Shivajinagar, Pune-5, India
Email: vhj.comp@coep.ac.in
[2] College of Engineering, Department of Electronics and telecommunication, Shivajinagar, Pune-5, India
Email: ppr.extc@coep.ac.in
[3] College of Engineering, Department of Computer Engineering and IT, Shivajinagar, Pune-5, India
Email: chandrama1684@gmail.com

***Abstract*—This paper presents a rotation scale invariant digital color image watermarking technique using Scale Invariant Feature Transform (SIFT) which is invariant to geometric transformation. The image descriptors extracted using SIFT transform of original image and watermarked image are used for estimating the scaling factor and angle of rotation of attacked image. Using estimated factors attacked image is then restored to its original size for synchronization purpose. As a result of synchronization, watermark detection is done correctly. In proposed approach the offline signature, which is a biometric characteristics of owner is embedded in second level detailed coefficients of discrete wavelet transform of cover image. The simulation results show that the algorithm is robust against signal processing and geometric attack.**

***Index Terms* — Biometric watermarking, Bi-Orthogonal wavelet , geometric attacks, SIFT**

I. Introduction

The rapid development of new information technologies has improved the ease of access to digital information. It also leads to the problem of illegal copying and redistribution of digital media. The concept of digital watermarking came up while trying to solve the problems related to the management of intellectual property of media. Access control or authenticity verification has been addressed by digital watermarking as well as by biometric authentication [2,3]. Recently, biometrics is adaptively merged into watermarking technology to enhance the credibility of the conventional watermarking technique. By embedding biometrics in the host, it formulates a reliable individual identification as biometrics possesses exclusive characteristics that can be hardly counterfeited. Hence, the conflicts related to the intellectual property rights protection can be potentially resolved [4]. Biometric watermarking is a special case of digital watermarking where the content of watermark or the host data (or both) are biometric entities. This imparts an additional layer of authentication to the underlying media [3].

Though novel and efficient watermarking algorithms have been developed, attempts also have been made by hackers to remove or destroy embedded watermark through various attacks. Among all attacks, especially geometric attacks are known as one of the difficult attack to survive. This is mainly due to the fact that slight geometric manipulation to the marked image desynchronizes the location of the watermark and causes incorrect watermark detection [4]. Geometric variation of watermarked media can induce synchronization errors between the extracted watermark and the original watermark during the detection process. It is very difficult to cope with geometric distortions especially for robust watermarking systems since these attacks break the synchronization between the watermark and detector.
Several approaches have been developed for synchronizing schemes, which can be divided into following categories.

- Use periodic sequence to embed the watermark in a repetitive pattern, allowing the detector to estimate the performed attack due to altered periodicities.
- Use of invariant-transform to maintain synchronization under rotation, scaling, and translation is the second approach. Examples of these transforms are log-polar mapping of DFT [8,9] and fractal transform coefficients [10], Fourier-Mellin transform, radon transform, Mexican Hat wavelet transform etc. Though these schemes are theoretically effective but difficult to implement due to poor interpolation accuracy during log-polar and inverse log-polar mapping.
- Template based approach to embed reference template to assist watermark synchronization during the detection process [11]. The template should be invisible and have low interference with the previously embedded watermarks.
- Moments based watermarking schemes makes use of magnitudes of Zernike moments as they are rotation invariant. Magnitudes of moments can be used as a watermark signal or be further modified to carry embedded data [3,14].
- Content based scheme is another solution for watermark synchronization. Media contents represent an invariant reference for geometric distortions so that referring to content can solve the problem of watermark synchronization, i.e., the location of the watermark is not related to image coordinates, but to image semantics [6].In this approach feature points are used as a content descriptor. The extracted feature of image content can be used for both watermark embedding and detection.

DOI: 01.IJSIP.03.01.80

Among all synchronization scheme, most promising class of synchronization method is feature based approach. In the proposed method Shift Invariant Feature Transform (SIFT) is used for synchronization purpose. SIFT is used to extract the feature points by considering local image properties and it is invariant to rotation, scaling, translation and partial illumination changes [12]. Feature points, which are also called as keypoints are localized elements of a cover image that are inherently linked to that image and usually contain semantic information. They have the property of being reasonably stable and are more difficult to remove by a malicious attacker. In this paper we propose a watermarking scheme which is resistant to geometric and signal processing attacks for color image. Feature points of original image and watermarked image are used for synchronization purpose at the time of watermark detection. These feature points are calculated by applying SIFT. Geometric manipulation is estimated by matching basic feature points of original image with attacked image. Offline hand written signature of owner is embedded as a watermark in second level detailed coefficients of discrete wavelet transform of cover object. The cover image is decomposed using biorthogonal wavelet transform. The rationale behind using handwritten signature as a watermark is that it is a socially accepted trait for authentication purpose and closely related with copyright holder.The paper is organized as follows: A brief review of SIFT is provided in section II. Section III provides the outline of the method employed and the results are provided in the next section. The last section summarizes the work and future scope.

II. SIFT

Feature points are elements of information inherently linked to the content. These local invariant features are highly distinctive and matched with a high probability against large image distortions. As a result, the relative position of such a feature point remains constant after an attack and hence it is suitable for synchronization.

Though numerous techniques can be applied for feature extraction, SIFT proposed by David Lowe [12] has proved to be very efficient. Even when the image is subjected to attacks like image zoom, rotate, brightness change and affine transform, the local features based on SIFT will not be changed. Considering the local image characteristics, SIFT operator extracts features and their properties such as the location (x,y), scale S, and orientation è. The basic idea of the SIFT is to extract features through a staged filtering that identifies stable points in the scale space by selecting candidates for features by searching for peaks in the scale space. In order to extract candidate locations for features, the scale space $D(x, y, \sigma)$ is computed using Difference of Gaussian (DoG) function as given by equation (1).

$$D(x, y, \sigma) = (G(x, y, k\sigma) - G(x, y, \sigma)) * I(x, y) \qquad (1)$$

Gaussian kernel successively smooths original images with a variable-scale σ and calculate the scale-space images by subtracting two successive smoothed images. The parameter is a variance, called a scale of the Gaussian function. In these scale space images, all local maxima and minima are retrieved by checking the closest eight neighbors in the same scale and nine neighbors in the scales above and below. These extrema determine the location (x,y) and the scale 'S' of the SIFT features, which are invariant to the scale and orientation change of images.

III. Proposed scheme

The proposed watermarking method embeds offline handwritten signature of the owner which is a biometric characteristic as a watermark in color image. The color image is separated into three channels red, blue and green. Red channel is used to extract feature points using SIFT and these feature points are saved as synchronous registration information which is required for watermark detection. As human eye is less sensitive to changes in blue color, we prefer to embed watermark in blue channel. Feature point extraction channel and watermark embedding channel are separated intentionally to achieve stable feature. The original image is not required for watermark detection but feature points are used to estimate geometric distortion. Thus, it is a semiblind algorithm. An offline hand written signature from the user is pre-processed and converted into a binary bit string before embedding.

The proposed scheme is carried out in four phases, watermark preparation, watermark embedding phase, the geometric attack estimation phase, and watermark detection phase. Fig.1 shows the block diagram of proposed watermarking scheme.

A. Watermark preparation

The offline handwritten signature of the owner which is used for authentication purpose is converted to a 1-D binary string through vector division with values ranging between 0 and 1 only. This is essential as watermarking will be done based on these two values only.

B. Watermark embedding

Watermark embedding consists of following steps:

1. Separate the colour carrier image into three colour channels.
2. Calculate feature points of red channel by using SIFT and save as synchronous registration information.
3. Perform 2-level DWT using bi-orthogonal wavelet transform on the blue and green components of carrier image.
4. Using a private key generate the pseudorandom sequence which is equal to the length of watermark.
5. Select the LH subband of blue and green channel of decomposed image and generate the perceptual mask that selects the wavelet coefficients from these bands. This is based on pseudorandom sequence using private key.
6. Embed the watermark in selected coefficients of blue component of the host image as based on following logic.

DOI: 01.IJSIP.03.01.80

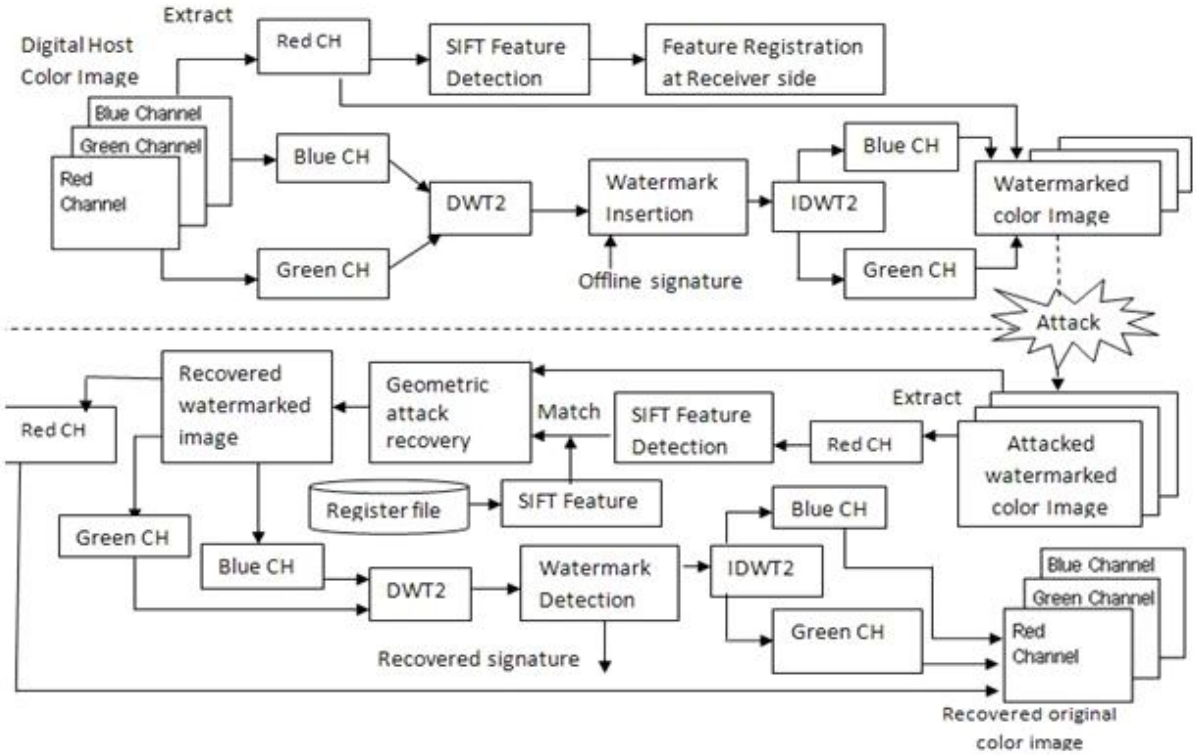

Figure1. Watermark embedding and extraction scheme

i) For entire length of watermark
ii) Compare blue channel coefficientswith green channel coefficients
iii) If Watermark bit is '1'
iv) Set blue channel coefficient to a value higher than corresponding green channel coefficient
v) Else if watermark bit is '0'
vi) Set blue channel coefficient to a value smaller than corresponding green channel coefficient
vii) End if
viii) End for
7. Reconstruct the watermarked image using inverse discrete wavelet transform

The offset value (OV) that is to be added or subtracted from green channel coefficients to make corresponding blue channel coefficients smaller or larger based on watermarking bits is given by

$$OV = \frac{Avg\_lum(I_b)/\sqrt{mxn}}{4} \quad (2)$$

Where Avg_lum is the intensity of blue component of image, m and n are the dimensions of image. Traditionally, offset value is fixed. In proposed scheme the offset is adapted depending upon the image. This results in better PSNR than fixed offset value.

C. Geometric attack estimation

Feature points can be used either for watermark embedding/detection or for synchronization. Our approach uses SIFT feature points for synchronization.It can estimate the geometric distortion by using feature points of both original and watermarked image. For estimation of geometric transform, we have considered the approach of [1].

a. Scale estimation and correction

Feature points are suitable for watermarking with implicit synchronization as those have covariance with geometric transformations.

$$S_{est} = \frac{\sum_{i=1}^{m} q_i}{\sum_{i=1}^{m} p_i} \quad (3)$$

Where 'm ' is the total number of matched feature points of original image and watermarked image, 'S' is the scaling factor of attacked watermark image, p_i and q_i are the scales of matched feature points of original and watermarked image. Scaling correction is done by resizing the attacked watermarked image by scale correction factor given by equation (4).

$$scale\_correction = S_{est}^{-1} \quad (4)$$

b. Rotation estimation correction

Angle of rotation of attacked image can be calculated based on orientation difference of matched feature points of original and attacked image. Assuming watermarked image is rotated by an angle 'è', total number of matched feature points as 'm', the centre angle of original image feature points as $\emptyset_o$ and that of corresponding matched feature point of rotated image as $\emptyset_r$,the estimation of angle by which watermarked image is rotated can be computed as follow:

DOI: 01.IJSIP.03.01.80

$$\theta_{est} = \frac{\sum_{i=1}^{m}(\emptyset_r - \emptyset_o)}{m} \quad (5)$$

The image is restored to its original shape by rotating it by anti rotation factor given by equation (6)

$$anti\_rotation = -\theta_{est} \quad (6)$$

D. Watermark detection.

In this stage, watermarked image is checked for any geometric distortions such as scaling, rotation or a combination of both. Watermark detection steps are as follow:

1. Segregate the three channels of watermarked colour image and extract the feature points of red channel using SIFT.
2. Synchronization step:

Compare these feature points with feature points of original image to estimation geometric distortion.

3. Correct these geometric distortions.
4. Apply 2 level wavelet transform using bi-orthogonal wavelet on blue and green channel
5. Using the private key, generate pseudorandom sequence equal to length of watermark which is used as perceptual mask.
6. Using perceptual mask identify the coefficients of blue and green channel from LH band of second level decomposition.
7. Watermark detection is based on following logic:

i) While length of watermark
ii) Compare blue channel coefficients with corresponding green channel coefficients
iii) If blue channel coefficient is higher than corresponding green channel coefficient
iv) Set watermark bit equal to one
v) Else if blue channel coefficient is smaller than corresponding green channel coefficient
vi) Set watermark bit equal to zero
vii) End if
viii) End while

8.Reshape it to form two dimensional signature image

E. Experimentation and results

The evaluation of proposed scheme is performed by keeping in mind that the embedded watermark should be invisible and fidelity of host image is maintained. Watermark data size is variable depending upon the size of the signature image, however the general range is in between 60 × 30 to 120 × 120.

Apart from the perceptual quality of the watermarked image and recovered watermark, the quantitative metrics used to evaluate the quality of watermarked image are PSNR and SNR, while that of recovered signature is Structural Similarity Index Measure (SSIM) [13].

TABLEI. PERCENTAGE OF ACCURACY OF ESTIMATED SCALE FACTOR

Scaling factor	Estimated scaling factor	Percentage of accuracy
0.5	0.5601	87.96
0.6	0.6526	91.22
2	2.0372	98.13
3	3.0351	98.82
4	4.0750	98.12
5	5.0804	98.39
6	6.1199	98.00

Standard images used for watermarking are Leena, Baboon, Pepper, Cameraman etc, while fourteen different signatures are taken as a watermark. Table I shows the actual scaling factor, estimated scaling factor and percentage of accuracy. Table II shows the angle by which image is rotated, estimated rotation angle and percentage of accuracy.

TABLEII. PERCENTAGE OF ACCURACY OF ESTIMATED ROTATION ANGLE

Rotation angle	Estimated rotation angle	Percentage of accuracy
10	9.94132	99.41
20	20.0890	99.55
30	29.8258	99.42
40	40.3002	99.25
60	59.3999	99
90	89.97069	99.97
100	100.1319	99.87
110	109.9108	99.92
120	119.4345	99.53
150	148.9016	99.27
170	169.5421	99.73
300	298.3983	99.47
330	330.9143	99.72

To verify the invisibility of embedded watermark, quality of watermarked image, quality of extracted watermark and robustness of scheme against various attacks rigorous simulation testing is carried out. A sample output of original image, watermarked image along with original and recovered watermark is shown in Fig. 2.The average PSNR of watermarked image without any attack is above 40dB. SSIM of extracted signature from watermarked image under different signal processing and geometric attack is tabulated in Table III. The perceptual quality of extracted signature is marked on a scale of three as good, recognizable and poor.

DOI: 01.IJSIP.03.01. 80

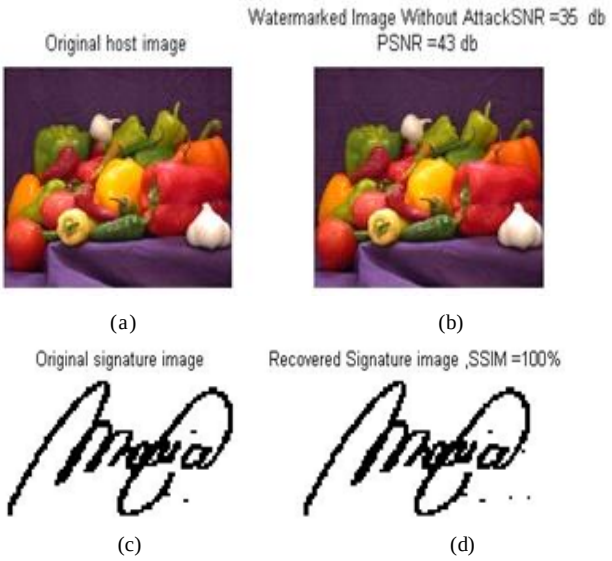

Figure 2 Watermarked image along with original and recovered watermark

A sample of watermarked image which is rotated by 120 degree and extracted watermark is shown in Fig. 3.

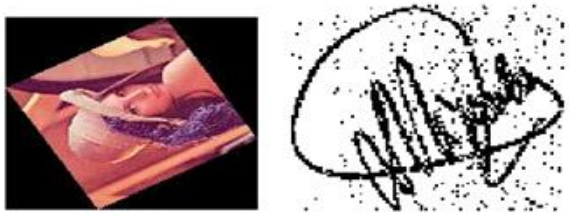

Figure3. Attacked watermarked image and extracted watermark

Some of the extracted signatures under different attacks are shown in Fig. 4

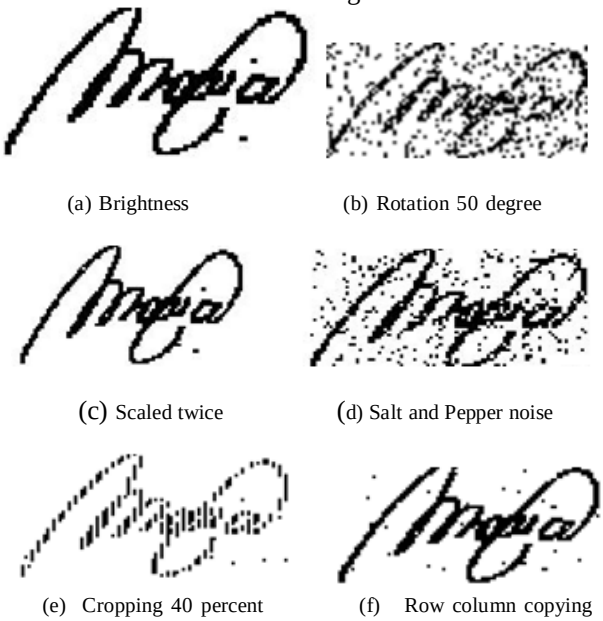

Figure4. Extracted watermarks under different attacks

TABLE III. SUMMARY OF ATTACKS

Type of attack	parameter	SSIM	Perceptual quality of recovered signature
Rotate	30^0	99.43%	Recognizable
	40^0	99.15%	Recognizable
	45^0	98.60%	Recognizable
	50^0	98.54%	Recognizable
	80^0	99.56%	Recognizable
	120	99.45%	Recognizable
Scale	0.5	99.68%	Good
	1	99.99%	Good
	2	99.99%	Good
	3	99.99%	Good
	4	99.99%	Good
Crop	10	99.99%	Good
	30	99.56%	recognizable
Brightness	5	99.24%	Good
Salt & Pepper	0.1	99.21%	recognizable
	0.2	98.65%	Recognizable
Row Column Copying	Random selection	100%	Good
Row Column Blanking	Random selection	100%	Good
Gaussian white noise	0.01	98.35%	Recognizable
	0.08	98.45%	Recognizable
JPEG	Q = 95	99.43%	Good
	Q = 90	99.61%	Good
	Q = 85	99.37%	Recognizable
	Q = 80	99.323%	Recognizable
Histogram equalization		94.30%	Poor

Conclusion and Future scope

The paper proposes a novel biometric watermarking technique using an amalgamation SIFT. The technique is highly robust against numerous geometric and signal processing attacks like cropping, scaling, rotation, median and Weiner filtering, Gaussian and salt and pepper noise, histogram equalization and JPEG compression.

The fidelity of watermarked image is highly maintained as PSNR is above 40dB. However, survival against a combination of geometric attack like scaling and rotation, shearing and scaling is still a challenge. The current study can be extended to develop watermarking scheme using RST invariant transform like Complex wavelet transform, Zernike moments or combination of both which is resilient to complex geometric attacks.

DOI: 01.IJSIP.03.01.80

REFERENCES

[1] Wei Yan, Yihong Hu, Guochu Shou, Zongjue Qian , "The Algorithm of Color Image Watermarking Based on SIFT," proceedings of IEEE international conference on e-Business and Information Security, 22-23 May 2010

[2] Cox I. Kilian , J. Leighton T.," Secure spread spectrum watermarking for multimedia ," IEEE Transaction on Image Processing ,vol. 6, pp.1673–1687,1997.

[3] Zheng, D., Liu, Y., Zhao, J., and El Saddik, "A survey of RST invariant image watermarking algorithms," ACM Computing Surveys vol. 39, no.2, Article 5 , June 2007

[4] Liu Jing1 , Liu Gang, Zhang Jiulong, "Robust Image Watermarking Based on SIFT Feature and Optimal Triangulation," 2009 International Forum on Information Technology and Applications

[5] Chih-Wei Tang and Hsueh-Ming Hang, "A Feature-Based Robust Digital Image Watermarking Scheme ," IEEE transaction on Signal Processing, vil. 51, no. 4, April 2003

[6] Hae-Yeoun Lee , Hyungshin Kim, Heung-Kyu Lee," Robust image watermarking using local invariant features ," Optical Engineering 45 (3), 037002 , March 2006

[7] M, Kutter," Watermarking resisting to translation , rotation and scaling," proc. SPIE 3528, 423-431,1998

[8] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, and Y. M. Lui, "Rotation, scale and translation resilient public watermarking for images," Proc. SPIE Security Watermarking Multimedia Contents II, vol. 3971, pp. 90–98, 2000.

[9] S. Pereira and T. Pun, "Robust template matching for affine resistant image watermarks," IEEE Transaction on Image Processing, vol. 9, pp. 1123–119, June 2000.

[10] Z. Ni,E. Sung, and Y. Q. Shi, "Enhancing robustness of digital watermarking against geometric attack based on fractal transform," in Proceeding IEEE International Conference Multimedia Expo., vol. 2, 2000, pp. 1033–1036

[11] S. Pereira and T. Pun, "Robust template matching for affine resistant image watermarks," IEEE Transaction on Image Processing, vol. 9, pp. 1123–1129, June 2000

[12] Lowe, D. G., "Distinctive Image Features from Scale-Invariant Key points," International. Journal of Computer Vision, 91-110 2004.

[13] Zhou Wang, Alan Bovik, Hamid Shaikh, Eero Simoncelli , "Image Quality Assessment: From Error Visibility to structural Similarity," IEEE Transaction on Image Processing, vol. 13, no. 4, April 2004

[14] Xiang-Yang Wang, Li-Min Hou," A new robust digital image watermarking based on pseudo-Zernike moments," Springer Multidimensional System and Signal Processing (2010) 21:179–196 DOI10.1007/s11045-009-0.

DOI: 01.IJSIP.03.01.80